Relationship between quantum repeating devices and quantum seals

Guang Ping He*
School of Physics & Engineering and Advanced Research Center,
Sun Yat-sen University, Guangzhou 510275, China

It is revealed that quantum repeating devices and quantum seals have a very close relationship, thus the theory in one field can be applied to the other. Consequently, it is shown that the fidelity bounds and optimality of quantum repeating devices for decoding quantum information can be violated when they are used for decoding classical information from quantum states, and the security bounds for protocols sealing quantum data exist.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.65.Ta, 03.67.Ac, 03.67.-a

I. INTRODUCTION

Suppose that many users share a single quantum communication channel in multiuser transmission. Each user decodes the transmitted information from the channel and passes the carrier to the subsequent user. In this case, they need a quantum repeating device [1] in which the information can be decoded reliably, while the quantum state of the carrier is expected to be optimally preserved. (Note that such a device was called as "quantum repeater" in Ref. [1], but the meaning differs from these in Refs. [2, 3]. To avoid confusion, we prefer not to use the term quantum repeater in this paper.) When quantum information is being transmitted, the information-disturbance tradeoff of the devices was intensively studied in literature [4, 5, 6, 7]. Optimal quantum repeating devices were also proposed in Refs. [1, 8, 9, 10]. Nevertheless, in most cases of quantum communication, a user generally cares little about the exact quantum state of the carrier. Instead, he only wants to know the classical information encoded in this quantum state. For example, in the well-known quantum key distribution (QKD) problem [11, 12, 13], a classical bit 0 (1) can be encoded as the quantum state $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$), where $|0\rangle$ and $|1\rangle$ are the two orthogonal states of a qubit and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. An eavesdropper is only interested in whether the classical content is 0 or 1. There is no need for him to distinguish $|0\rangle$ from $|+\rangle$ or $|1\rangle$ from $|-\rangle$. Therefore, it is more important to study the tradeoff between classical information gained versus quantum disturbance in quantum cryptography and search for optimal quantum repeating devices for this purpose.

On the other hand, quantum seal (QS) is a relatively less-known quantum cryptographic problem. Its goal can be summarized as follows. The owner of the secret data to be sealed (denoted as Alice) encodes the data with quantum states. Any reader (denoted as Bob) can decode the data from these states without the help of Alice. Meanwhile, if data has been decoded, it should cause a disturbance on the states, which is detectable by Alice. A QS protocol is considered to be secure if Bob cannot read the data while escaping Alice's detection simultaneously. QS can be classified by the types and the readability of the sealed data. If the data are a single classical bit, it is called quantum bit seals (QBSs). Else, if data are a classical string, it is called quantum string seals (QSSs). If data can always be retrieved by the reader with certainty, it is called a perfect QS. Else, if data can only be retrieved with a non-vanished error rate, it is an imperfect QS. The first perfect QBS protocol was proposed by Bechmann-Pasquinucci [14], but then it was found that all perfect QBS protocols are insecure against collective measurements [15]. Shortly later, it was proven that imperfect QBS also has security bounds [16]. Nevertheless, it was proven that secure imperfect QSS protocols exist [17, 18, 19, 20]. (Note that it was claimed in Ref. [21] that all QSS protocols are insecure. But as indicated later in Ref. [18], the cheating strategy proposed in Ref. [21] is not a successful cheating because it cannot obtain nontrivial amount of information while escaping the detection simultaneously [18, 19]. It was also realized in Ref. [20] that when the cheating in Ref. [21] escapes the detection, the ratio between the amount of information obtained by the cheater and that of the sealed string is arbitrarily small as the length of the string increases.) More intriguingly, it was proposed in Ref. [17] that secure QSS can be utilized to realize a kind of QBS, which is secure in practice. Very recently, it was found [22] that QS has a very close relationship with quantum bit commitment [23], which is another primitive of quantum cryptography.

Though the theories of quantum repeating devices and quantum seals are developed independently in literature, we can see that they are closely related since they both focus on the information-disturbance tradeoff on quantum systems. In the next section, we will show the rigorous equivalence between their parameters. As the examples of the application of this equivalence, we will apply the existing theory of QS to study quantum repeating devices and obtain interesting results on their fidelity bounds and optimality in Sec. III. Also, we will apply the existing theory of quantum repeating devices in Sec. IV, to study the security bounds for QS protocols sealing quantum data.

*Electronic address: hegp@mail.sysu.edu.cn

II. EQUIVALENCE BETWEEN QUANTUM REPEATING DEVICES AND QUANTUM SEALS

A. Theory of quantum repeating devices

Let us review briefly the description of quantum repeating devices in Refs. [1, 8]. Suppose that an input state $|\psi\rangle$ reaches a user via a quantum communication channel. This user not only wants to decode the information of the state for himself alone, but also wants to leave the state less disturbed so that the subsequent user(s) can also decode some information of the state without his help. For this purpose, he runs a device which accomplishes the following tasks:

(i) A certain positive operator-valued measurement (POVM) $\{\Pi_k\}$ is performed on $|\psi\rangle$.

(ii) When the outcome k is observed at the output of the device, he uses an inference rule $k \rightarrow |\phi_k\rangle$ to obtain the estimated signal state $|\phi_k\rangle$ as an approximation of the input state $|\psi\rangle$. Note that the exact form of $|\phi_k\rangle$ should be known to the user. That is, e.g., when $|\phi_k\rangle$ is a qubit $x\,|0\rangle + y\,|1\rangle$, he should know the values of x and y.

(iii) After the POVM, a conditional state $|\psi_k\rangle$ (whose form depends on the value of k) is left to the subsequent user(s) for further decoding.

Such a device is the quantum repeating device that we are referring to. From this description, we can see that it is closely related with the well-known quantum cloning machine [24], whose purpose is also to transform an input state $|\psi\rangle$ into two (or more) output states $|\phi_k\rangle$ and $|\psi_k\rangle$. The difference is that at the end of the quantum cloning, the exact form of $|\phi_k\rangle$ can still be left unknown to the user. He may only own a quantum system whose state is $|\phi_k\rangle$. That is, a quantum repeating device can be viewed as a quantum cloning machine plus a measurement on the output state $|\phi_k\rangle$.

A user can choose the POVM at his will to construct his specific quantum repeating device. Different choices will result in different output states $|\phi_k\rangle$ and $|\psi_k\rangle$, which determine the quality of the device. Therefore it is natural to seek for the choice which can optimize this quality. There are two important parameters characterizing the quality of quantum repeating devices, i.e., the transmission F and estimation fidelities G. Generally, we are interested in the case where the possibility distribution of the input state looks completely random to the user. In this case, the corresponding fidelities for the given input signal $|\psi\rangle$, averaging over all possible outcomes, are defined as [1, 8]

$$F_\psi = \sum_k p_k \left|\langle\psi\,|\psi_k\rangle\right|^2 , \tag{1}$$

and

$$G_\psi = \sum_k p_k \left|\langle\psi\,|\phi_k\rangle\right|^2 . \tag{2}$$

Here, p_k denotes the probability for the outcome k to be observed at the output of the quantum repeating device, so that the input state $|\psi\rangle$ is decoded as the estimated signal state $|\phi_k\rangle$, while the state $|\psi_k\rangle$ is left to the subsequent user. Performing average over all possible input states $|\psi\rangle$, i.e., over the alphabet A of transmittable symbols (states), the transmission fidelity F and the estimation fidelity G are given, respectively, by

$$F = \int_A d\psi F_\psi \tag{3}$$

and

$$G = \int_A d\psi G_\psi . \tag{4}$$

Some bounds on the values of F and G of different quantum repeating devices were already found. Consider two extreme cases. In the case where nothing is done by the quantum repeating device, the input state is passed to the subsequent user unaltered and thus $F = 1$. Meanwhile, the outcome has to be estimated by guess, thus $G = 1/d$, where d is the dimension of the Hilbert space of the input states. In the opposite case where the quantum repeating device gains the optimal information from the input state so that the final state left to the subsequent user cannot provide any information on the initial state, it was shown that $F = G = 2/(d+1)$ [5, 6]. Therefore we have

$$2/(d+1) \leq F \leq 1 \tag{5}$$

and

$$1/d \leq G \leq 2/(d+1). \tag{6}$$

In general cases where the quantum repeating device provides only partial information while partially preserving the quantum state of the input signal for the subsequent user, a tighter bound between F and G was found [7] for randomly distributed input signals, i.e.,

$$\begin{aligned} & (F-F_0)^2 + d^2(G-G_0) + \\ & 2(d-2)(F-F_0)(G-G_0) \\ \leq\ & (d-1)/(d+1)^2, \end{aligned} \tag{7}$$

where $F_0 = (d+2)/[2(d+1)]$ and $G_0 = 3/[2(d+1)]$. For two-dimensional Hilbert space, the bound reduces to

$$(F-2/3)^2 + 4(G-1/2)^2 \leq 1/9. \tag{8}$$

B. Theory of quantum seals

The model of QBS (i.e., the protocols sealing a single classical bit) was established in Ref. [16]. By analogy, here we establish a general model of QS (i.e., covering the protocols sealing any kind of classical bit(s), strings, or quantum information) as follows:

(1) Alice, who owns the information b to be sealed, maps b into a certain quantum state $|\phi \otimes \psi\rangle$ of the system $\Phi \otimes \Psi$ and keeps the system Φ to her own while making Ψ accessible by any potential reader Bob who may want to decode b.

(2) Alice lets Bob know an operation P for decoding. If the state of Ψ is an eigenstate of P, the protocol is a perfect QS. Otherwise it is an imperfect QS.

(3) Alice lets Bob know a series of sets G_i's and a series of values b_i's, which satisfies $G_i \cap G_j = \emptyset$ $(\forall i \neq j)$, such that if he applies P on Ψ and the outcome g belongs to set G_i, he should take the value of the sealed data as $b' = b_i$; while if g does not belong to any G_i, the sealed information cannot be identified, i.e., Bob needs to guess b' by himself. (In the case where the sealed information b is a quantum data, each b_i should be understood as a set of parameters sufficient to describe a quantum state.) Note that since the state of Ψ may not be an eigenstate of P, the value of b' thus obtained will match Alice's input b with a certain probability only. Let α denote the average of this probability over all possible b and b', which measures the readability of the protocol.

(4) At any time, Alice can access to the entire system $\Phi \otimes \Psi$ and compare its current final state $|\phi' \otimes \psi'\rangle$ with the initial state $|\phi \otimes \psi\rangle$. Therefore, if b has been read, Alice can detect it with the probability $1 - |\langle \phi \otimes \psi|\ \phi' \otimes \psi'\rangle|^2$. Let β denote the average of this probability over all possible initial and final states, which measures the security of the protocol.

For QBS, b is limited to a single classical bit. In this case, it was shown [16] that the parameters α and β in such a protocol must satisfy the following security bounds:

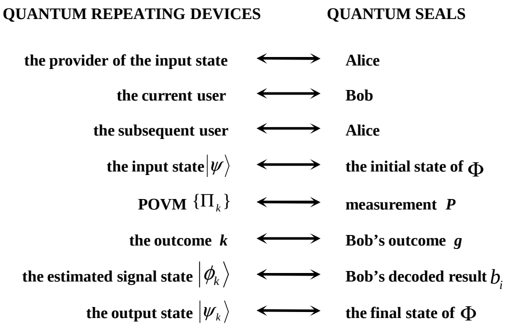
$$\beta \leq 1/2 \tag{9}$$

and

$$\alpha + \beta \leq 9/8. \tag{10}$$

C. Equivalence

By comparing the above descriptions, we can see the relationship between the two subjects. Suppose that Alice encodes a certain information with a quantum state $|\psi\rangle$, Bob decodes the information from $|\psi\rangle$ with a quantum repeating device suggested by Alice, and the resultant state $|\psi_k\rangle$ is acquired later by Alice to detect whether the information has been decoded. Then the quantum repeating device in fact fulfills an embodied implementation of quantum seals. On the contrary, Alice can use a quantum seal protocol to encode some information on a quantum system Ψ and send it to Bob via the quantum communication channel, Bob decodes it with the operation P suggested by the protocol, and another subsequent user instead of Alice receives the final state of the system Ψ for further decoding. Then the quantum seal works as a quantum repeating device in this case. Therefore, quantum repeating devices and quantum seals are in fact equivalent. That is, we can set up a mapping between the elements of the two subjects as shown in Fig. 1. Then a scheme for quantum repeating device can be constructed from a quantum seal protocol and vice versa.



QUANTUM REPEATING DEVICES		QUANTUM SEALS
the provider of the input state	⟷	Alice
the current user	⟷	Bob
the subsequent user	⟷	Alice
the input state $|\psi\rangle$	⟷	the initial state of Φ
POVM $\{\Pi_k\}$	⟷	measurement P
the outcome k	⟷	Bob's outcome g
the estimated signal state $|\phi_k\rangle$	⟷	Bob's decoded result b_i
the output state $|\psi_k\rangle$	⟷	the final state of Φ

FIG. 1: The equivalence between the elements of quantum repeating devices and quantum seals.

Consequently, there is a rigorous quantitative relationship between the parameters F, G and α, β describing the quality of quantum repeating devices and quantum seals, respectively. Since the input and output states $|\psi\rangle$ and $|\psi_k\rangle$ and the user's estimated signal state $|\phi_k\rangle$ of quantum repeating devices are equivalent to the initial and final states of the system Ψ and Bob's decoded result b_i of quantum seals, respectively, by the definitions of the parameters F, G and α, β, we yield

$$F = 1 - \beta \tag{11}$$

and

$$G = \alpha. \tag{12}$$

Nevertheless, we should note that the existing theories of quantum repeating devices and quantum seals focus on different species of information-disturbance tradeoff. On one hand, the existing theory of quantum repeating devices generally studies merely the case where the user wants to decode the *quantum* aspect of the information encoded in the quantum states. The case where the user tries to decode only the *classical* information encoded in the quantum states was left out in literature. But as mentioned in Sec. I, in many practical communication settings including QKD, an essential problem is that an eavesdropper wants to know the classical information only. That is, he needs not to distinguish the quantum states exactly, as long as these states are corresponding to the same classical information. Therefore the existing theory of quantum repeating devices contributed less to the security analysis of quantum communication. On the other hand, the security of protocols sealing *classical* information (either strings or a single bit) was well studied in literature, while it still remains unclear how (in)secure the protocols sealing *quantum* information can be. For this reason, our current finding on the equivalence between quantum repeating devices and quantum seals is instructive. It indicates that we can apply the existing theories interchangeably and find interesting results for both fields. In the following, we will present some examples.

III. FIDELITY BOUNDS AND OPTIMALITY OF QUANTUM REPEATING DEVICES FOR CLASSICAL INFORMATION

In this section, we will use the security bounds of quantum seals to find interesting results on quantum repeating devices. Consider the quantum repeating device decoding one single bit of classical mutual information from quantum states. In this case, the bound (10) applies. Using Eqs. (11) and (12), it can be rewritten as

$$G-F\leq 1/8. \tag{13}$$

Note that in this case, G is the estimation fidelity of the decoded *classical* (instead of quantum) information. Therefore the bound (6) obtained in the quantum case is not necessarily applied. Consequently, the bounds (7,8) no longer exist. Indeed, when $G-1/2>1/6$, i.e., $G\geq 2/3$, we have

$$(F-2/3)^2+4(G-1/2)^2\geq 4(G-1/2)^2>1/9. \tag{14}$$

This inequality holds for any dimension d because Eq. (10) and its derivative Eq. (13) are valid regardless the dimension of the Hilbert space of the input states. In the $d=2$ case, i.e., the input state is a qubit, Eq. (14) clearly shows that the quantum bound (8) is surpassed for any quantum repeating device which can decoded one classical bit of mutual information from the input quantum states with the estimation fidelity $G\geq 2/3$. Such a value of G can indeed be reached in real settings. For example, in the original BB84 QKD protocol [11], the quantum states $|0\rangle$ and $|+\rangle$ both encode the classical bit 0, while the states $|1\rangle$ and $|-\rangle$ both encode 1. Then a quantum repeating device can be designed as follows. Measure the input states in the Breidbart basis [25], i.e., $\{\cos(\pi/8)|0\rangle+\sin(\pi/8)|1\rangle,\cos(5\pi/8)|0\rangle+\sin(5\pi/8)|1\rangle\}$, and output "0" ("1") if the measurement result is $\cos(\pi/8)|0\rangle+\sin(\pi/8)|1\rangle$ $(\cos(5\pi/8)|0\rangle+\sin(5\pi/8)|1\rangle)$. In this case, randomly distributed input bits can be decoded with the estimation fidelity $G=\cos^2(\pi/8)\simeq 0.8536>2/3$.

One of the significance of this result is that it indicates that the security of quantum communication channel needs to be evaluated more conservatively. This is because the transmission fidelity F, being the measure on how well the input quantum state is preserved, is related directly to the probability of detecting the eavesdropper who uses the quantum repeating device to decode information on the state. Higher F means less successful probability of the detection. Therefore Eq. (14) surpassing Eq. (8) means that F can be higher for the same G if the eavesdropper decodes only the classical information instead of trying to know the exact form of the input quantum state. Such a case is exactly what the eavesdropper does in most quantum communication we are interested today (e.g., QKD). Therefore Eq. (13) will be more appropriate than Eqs. (7,8) for evaluating the security of such quantum communication channels.

Another question immediately followed is whether optimal quantum repeating devices for decoding quantum information [i.e., whose F and G saturate the bounds (7,8), for example, the schemes proposed in Ref. [1]] are still optimal for decoding classical information. Before giving an answer, we must notice what "optimal" means in the latter case. As shown above, when the purpose of the quantum repeating device is to decode a classical bit only, the quantum bound (6) is gone. It was proven in Ref. [15] that perfect quantum seals can reach $\alpha=1$ and $\beta=0$ simultaneously. Therefore, using such quantum seals as the schemes of quantum repeating devices can reach $F=G=1$. That is, if by "optimal" we want to favor all users so that each of them can decode the bit with an estimation fidelity as high as possible, while leaving the carrier as less disturbed as possible, there exist perfect quantum repeating devices. But in this case, the quantum communication channel is trivial. This is because such perfect quantum repeating devices, being a direct analog of perfect quantum seals, will then have to encode different values of classical bits with orthogonal quantum states [15]. Since no nonorthogonal states are necessary, the channel can be completely classical. For example, simply writing a bit on a piece of paper and passing it through all the users can reach $F=G=1$. In this sense, the quantum repeating devices saturating the bounds (7,8) are surely not optimal for decoding classical information.

Here we consider another meaning of optimal. That is, our purpose is changed into trying to saturate the bound (13) to find a balance between a high-estimation fidelity G and a low-transmission fidelity F. Since a lower F means a higher β, our purpose means to find the balance of detecting eavesdroppers with a high probability, while still keeping the encoded bit highly readable. [Note that we do not want the quantum repeating devices that can saturate the bound (9) because it is indicates in Ref. [16] that the input states must contain zero amount of information of the encoded bits to saturate this bound.] Optimal quantum repeating devices for decoding quantum information are also not necessarily optimal for this purpose. This is because, as shown above, the bound (13) can violate the bounds (7,8) for certain values of G. On the other hand, In Ref. [16], an optimal scheme of quantum seals that saturates the bound (10) was proposed. Namely, Alice should seal the bit b in the form

$$\begin{aligned}|\phi_b\otimes\psi_b\rangle &= \frac{\sqrt{3}}{2}\sum_i c_{b,i}^{(b)}\left|\hat{f}_i^{(b)}\right\rangle\left|\hat{e}_i^{(b)}\right\rangle \\ &\quad +\frac{1}{2}\sum_i c_{b,i}^{(\bar{b})}\left|\hat{f}_i^{(\bar{b})}\right\rangle\left|\hat{e}_i^{(\bar{b})}\right\rangle. \end{aligned}\tag{15}$$

Here $\left|\hat{f}_i^{(b)}\right\rangle$'s ($\left|\hat{e}_i^{(b)}\right\rangle$'s) are the orthogonal states of Alice's system Φ (Bob's system Ψ) corresponding to the sealed bit b, with $c_{b,i}^{(b)}$'s being the superposition coefficients. This scheme has $\alpha = 3/4$, $\beta = 3/8$ thus reaches $\alpha + \beta = 9/8$. Therefore, optimal quantum repeating devices for decoding classical information can be designed accordingly.

As a simplified example, suppose that in a quantum communication channel, the classical bit 0 is encoded as either $(\sqrt{3}/2)\left|0\right\rangle + (1/2)\left|1\right\rangle$ or $(\sqrt{3}/2)\left|0\right\rangle - (1/2)\left|1\right\rangle$ and 1 is encoded as either $(1/2)\left|0\right\rangle + (\sqrt{3}/2)\left|1\right\rangle$ or $(1/2)\left|0\right\rangle - (\sqrt{3}/2)\left|1\right\rangle$. Then the optimal quantum repeating device is to measure the input states in the basis $\{\left|0\right\rangle, \left|1\right\rangle\}$, and output "0" ("1") if the measurement result is $\left|0\right\rangle$ ($\left|1\right\rangle$). It can saturate the bound (13) for randomly distributed inputs.

Interestingly, the encoding method of the original BB84 QKD protocol cannot allow quantum repeating devices saturating the bound (13). As calculated above, the best estimation fidelity is $G = \cos^2(\pi/8)$. According to Eq. (9) of Ref. [16], it can be calculated that the transmission fidelity is $F = 1 - 2G(1 - G) = 3/4$, therefore we have $G - F \simeq 0.1036 < 1/8$ in this case. It will be interesting to study what advantages can be brought when the optimal encoding method suggested by Eq. (15) is adopted in QKD or other quantum cryptographic task.

IV. SECURITY BOUNDS FOR SEALING QUANTUM DATA

Ever since the first proposal of the concept of quantum seals, it became a major problem whether unconditionally secure quantum seals exist. As reviewed in Sec. I, the security of the protocols sealing classical data was already studied thoroughly [15, 16, 17, 18, 19, 20]. For the case where the sealed information is quantum data, a protocol was proposed in Ref. [26], but later found insecure by the author himself. However, to date, there is still a lack of a general conclusion on the exact security bound of the protocols sealing quantum data. Here, with the equivalence between quantum seals and quantum repeating devices, we can study the problem with the theory of the latter.

Before we proceed, it is important to note that it makes a major difference whether the quantum data to be sealed is known to Alice or not. If the quantum data are known to Alice, then the problem is in fact equivalent to the sealing of classical information. Alice can simply use a classical string to describe how to prepare a quantum system whose state contains the quantum data to be sealed and seal this classical string with QSS protocols such as the one proposed in Ref. [17]. With this method, even sealing a single qubit can be secure. This is because for a qubit $\left|\psi\right\rangle = \cos\theta\left|0\right\rangle + \sin\theta\left|1\right\rangle$, the value of θ can have infinite possibilities. It differs from the sealing of a single classical bit, where the sealed bit b can only have two possible values 0 and 1. Therefore the insecurity proof of QBS [16] does not apply to this case. On the contrary, from the security proof of QSS [17] it can be seen that if Bob wants to decode θ with the reliability $\alpha \to 1$, the probability for him to be detected will be $\beta \to 1$ thus the protocol is secure.

Now let us focus on the case where the quantum data to be sealed are unknown to Alice. To be rigorous, we further assume that Alice has only one single copy of the quantum system containing these data, so that her knowledge on the data is minimized. Let us apply the theory of quantum repeating devices in this case. By combining Eqs. (5) and (11), we can see that any QS protocol using a d-dimensional state to seal quantum data is bound by

$$\beta \leq 1 - 2/(d + 1). \tag{16}$$

It means that when the sealed data are a quantum state in a high-dimensional Hilbert space ($d \to \infty$), the existing theory provides little limitation on the detecting probability β. Thus, a properly designed protocol may reach $\beta \to 1$ when sealing a high-dimensional quantum state and therefore can be regarded as secure. On the other hand, the security level of QS for low-dimensional quantum states is bound significantly by the dimensionality d. Especially, when $d = 2$, we have

$$\beta \leq 1/3. \tag{17}$$

Note that even when the sealed data are a qubit, the quantum state used to seal it is not necessarily a two-dimensional state. If the sealed qubit is mapped into a high-dimensional state and, most important of all, if there is a method to force Bob to decode other abundant information when he wants to decode the sealed qubit, then QS protocols sealing a qubit can be made secure. Nevertheless, so far we cannot prove the existence of this method. Therefore, before such a method can be found in future researches, the security of QS sealing a single qubit has to be bound by Eq. (17). That is, when Bob decoded the sealed qubit, Alice stands only 1/3 chances to detect it. Comparing to the security bound of QS sealing a single classical bit [16] (i.e., $\beta \leq 1/2$), sealing a qubit is even less secure.

At last, we would like to note that Eqs. (7) and (8) cannot immediately give an analog of Eq. (10) for QS protocols sealing quantum data. This is because there is still a subtle difference between QS and quantum repeating devices. According to feature (2) of the above model of QS, Alice should provide Bob with an operation P for decoding. This operation can generally enhance the reliability α of data decoded by Bob (unless Alice wants to mislead Bob to the wrong outcome in the QS protocol). On the other hand, in the quantum repeating device problem, Eq. (6) was obtained without assuming the existence of such a suggested operation. Therefore in QS protocols sealing quantum data, G (i.e., α) is not restricted by Eq. (6) and therefore the bounds in Eqs.

(7) and (8) may be surpassed. Exact bounds of G will depend on the details of the operation P and vary for different protocols.

V. SUMMARY

Thus it is shown that the transmission fidelity F and the estimation fidelity G describing the quality of quantum repeating devices are related directly to the readability α and the detecting probability β of quantum seals. Therefore, the theory in one field can be applied to the other. With this method, we found that the existing fidelity bounds Eqs. (7,8) of quantum repeating devices for decoding quantum information can be surpassed when they are used for decoding classical information from quantum states. Instead, the bound in the latter case is Eq. (13). Also, optimal quantum repeating devices for quantum information are not necessarily optimal for classical information. We also found that the security of protocols sealing quantum data is bounded by Eqs. (16,17).

We thank Professor Matteo G. A. Paris for helpful discussions. The work was supported in part by the NSF of China under Grant No. 10605041, the NSF of Guangdong province, and the Foundation of Zhongshan University Advanced Research Center.

[1] M. G. Genoni and M. G. A. Paris, Phys. Rev. A **71**, 052307 (2005).

[2] H. -J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[3] W. Dür, H. -J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[4] R. Derka, V. Bužek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).

[5] D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).

[6] A. Acín, J. I. Latorre, and P. Pascual, Phys. Rev. A **61**, 022113 (2000).

[7] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).

[8] M. G. Genoni and M. G. A. Paris, J. Phys.: Conf. Ser. **67**, 012029 (2007).

[9] S. Olivares and M. G. A. Paris, J. Phys. A **40**, 7945 (2007).

[10] M. G. Genoni and M. G. A. Paris, Phys. Rev. A **74**, 012301 (2006).

[11] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[12] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[13] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[14] H. Bechmann-Pasquinucci, Int. J. Quantum Inf. **1**, 217 (2003).

[15] H. Bechmann-Pasquinucci, G. M. D'Ariano, and C. Macchiavello, Int. J. Quantum Inf. **3**, 435 (2005).

[16] G. P. He, Phys. Rev. A **71**, 054304 (2005).

[17] G. P. He, Int. J. Quantum Inf. **4**, 677 (2006); quant-ph/0502091.

[18] G. P. He, Phys. Rev. A **76**, 056301 (2007); quant-ph/0602159v1.

[19] M. Nakanishi, S. Tani, and S. Yamashita, *Proceedings of the Sixth WSEAS International Conference on Information Security and Privacy (ISP'07)* (WSEAS, Puerto De La Cruz, Tenerife, Spain, 2007), p. 30.

[20] H. F. Chau, Phys. Rev. A **76**, 056302 (2007).

[21] H. F. Chau, Phys. Rev. A **75**, 012327 (2007).

[22] G. P. He and Z. D. Wang, arXiv:0804.3531v1.

[23] G. P. He, Phys. Rev. A **74**, 022332 (2006), and references therein.

[24] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[25] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology: Proceedings of Crypto '82* (Plenum Press, 1982), p. 267.

[26] H. F. Chau, quant-ph/0308146.